THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Cybercrime and Organizational Policies: A Survey of Cybercrime Cases in Kenya

Mitende Nicholus Nyapete
Lecturer, Department of Computer Science, St. Pauls University, Kenya
Dr. Ogalo, James Ochieng
Lecturer, Faculty of Information Science and Technology, Kisii University, Kenya

Abstract:
This study explores cases of cybercrime and discusses the need for national-level and organizational strategies to effectively combat the menace. Cyber threats have become so persistent; the attacks so pervasive, that organization and their leaders have essentially become inured to cyber security and an ever-increasing threat. The study reviewed existing literature and recent cases of cybercrime in Kenya and beyond to drive the focus of this paper. Common cases revealed that organizations fall victim to cyber-attacks, only then do they realize the time to take action was yesterday. In conclusion, security experts must move from their traditional reactive nature to a more proactive one. Equal priority should be on automated systems which detects the vulnerabilities as they occur, and also enable the systems to remediate these vulnerabilities immediately, before the damage occurs. Prosecutors, Law enforcement authorities, and judiciary, require developed framework, sustainable mechanisms, comprehensive technical support and solid platform for the investigation to cybercrime. The study recommended that for the digital evidence to see the light of the day in a court of law, the evidence process of acquisition, preservation, and analysis in a forensically safe manner and thus enable its presentation in court, specific equipment and software are needed and personnel and professionals concerned must be trained to recognize, properly understand, and examine the evidence presented.

Keywords: *Cybercrime, ICT infrastructure, organizational policies, crime investigation*

1. Background of the Study

With the everlasting quest for an improved ICT infrastructure, cybercrime has also risen tremendously and firms are also tasked to develop strategies to minimize these threats. In the course of time cybercrime has developed and changed, so did crime investigation techniques. In the recent times the need for investigating crime in a more accurate way has introduced forensic science, focusing on the collection and examination of evidence connected to a crime. The advancement of computing and Internet technologies has broadened the means of committing a crime. It was posited by Grabosky and Smith (1998) in reference to a notorious American bank robber who, when asked why he persisted in robbing banks, replied: "Because that's where the money is." Linking this flow of logic to the significance Asia possesses in terms of Internet users, one might grimly conclude that Asia will have to face a dark future in cyberspace, having the biggest number of cybercrime cases than anywhere in the world.

In recent years, cyber-crime has become increasingly sophisticated, making it difficult to combat, detect and mitigate. The rise of a relatively new class of cyber-attack is especially troubling. This new class is referred to as an (APT) 'Advanced Persistent Threat' (Rohini Tendulkar, 2013).

The Council of Europe's Convention of Cybercrime, which is to date the only international convention related to the issue that is legally binding, uses 'cybercrime' as an umbrella term to refer to an array of criminal activity including the following: offenses against computer data and systems, computer-related offenses, content offenses, and copyright offenses (Jaishankar, 2008).

Cyber-attacks do not only target technological vulnerabilities, but vulnerabilities arising from the behaviour of staff, suppliers and clients. Even with robust cyber-security measures in place, a single organization may find it difficult to control the cyber-security practices of its suppliers and any outsourced services. (Barney Jopson, 2013).

According to Wall (2007), the term 'cybercrime' itself is fairly meaningless since it was largely an invention of the media and thus has been used metaphorically and emotionally rather than scientifically or legally. Rather, he argued that the term cybercrime has a greater meaning if we construct it in terms of the transformation of criminal or harmful behavior by networked technology, rather than simply the behavior itself (Wall, 2007).

The spending in information technology infrastructure does not appear to be keeping up with emerging counter threats. Technology's influence has tremendously grown, with many firms adopting mobile solutions, social media, alternative workplace solutions, collaborative product innovation, digitized operations. This is happening amid a corresponding increase in regulatory controls associated with privacy controls, health information controls, financial data controls, intellectual property protection, and financial statement controls, and more. It's also happening at a time of increased awareness of cyber-campaigns targeting specific industries and organizations, and by adversaries who move from on-line industrial espionage to acts of destruction.

Business enterprises focus should be on the factors that can adversely affect an organization's cyber security and such considerations should be on; Strategy and execution of the cyber security program; Understanding changes in the threat environment; Identifying key organizational assets in need of protection; and Spreading that protection beyond the walls of the entity to encompass the enterprise ecosystem. As computer crime originating in the United States often implicates interstate and international laws, many cases fall under federal jurisdiction. Federal collaboration with local law enforcement and prosecutors to share intelligence and efforts through teamwork has demonstrated effectiveness in addressing traditional crimes involving drugs, weapons, gangs, and violence (McGarrell& Schlegel, 1993; Russell-Einhorn, 2004).

Money laundering with the use of computers concerns the process of concealing the source of illegally-obtained money and often involves the creation, fabrication, or alteration of documents to create a legitimate paper trail and history (Lyman, 2002). Financial institutions are presumed to keep detailed records of all transactions, currency exchanges, and the international transportation of funds exceeding a certain amount.

According to the press released by the cabinet secretary of Information, Communication and Technology Cabinet Secretary, Fred Matiangi, released the statistics during a conference that brought together stakeholders from the information and communication technology sector and the Communication Commission of Kenya(CCK) in Nairobi. "It is estimated that Kenya will by the end of this year lose nearly KES 2 billion (US$22,988,506) through fraud associated with all forms of cybercrime," said Matiangi during the session. The statistics further indicated that close to 1 000 Kenyans fall victim to internet fraud on daily basis. (Standard Newspaper pg.8, 2014). This evidence calls for a more solid cyber security infrastructural surveillance and advanced defenses.

Kenya has prepared itself to fight cybercrime in a stricter way than ever before by introducing a new internet monitoring device. Installed by the Kenya's Communication Commission (CCK), the monitoring device will help in detection and prevention of cyber-crime cases across the East African country. (Standard newspapers, 2012).

Although preparation is made to fight cybercrime, still new scenarios are increasingly emerging, making it difficult to criminalize this cases in a court of law. One of the evident report by standard news, thieves (cyber criminals) have complicated the cases and made it difficult to know the real identities of these criminals out of 22 cases out of 54 reported cases. Some cases are mysterious because they involve fraudulent transactions using cheques yet a suspect goes unidentified. For instance, one case involves a cheque paid to commissioner of taxes for clearance of goods used to clear goods for a different company yet the suspects are not known. The amount involved in this case was sh. 1.2 million. (The Standard newspaper, 2014).

Information theft continues to represent the highest external cost, followed by the costs associated with business disruption. Furthermore, compressive measures both legal, policies and surveillance techniques to sustain business continuity is of the essence.

2. Statement of the Problem

Cyber threats have become so persistent, the attacks so pervasive, that organizations and their leaders have essentially become inured to cyber security and an ever-increasing threat. When organizations fall victim to cyber-attacks, only then do they realize the time to take action was yesterday.

According to the report of the standard newspaper, Kenyan banks lost more than Kshs. 137 million to fraudsters in month of May, 2014 alone reported by banking fraud investigation department report. The report shows that fraudsters are increasingly becoming sophisticated with little chance of being caught or convicted in courts. The institutions targeted that month include first community bank, Barclays bank of Kenya, Equity Bank, Paramount Universal Bank and Kenya Commercial Bank, Cooperative Bank of Kenya, Commercial Bank of Africa, CFC Stanbic Bank, Habib AG Zurich Bank, National Bank, Consolidated bank and family bank. Only sh. 26,095,074 was recovered, representing recovery success rate of only 19 per cent. (The Standard newspaper, 2014).

"Put simply, relatively few Internet-related crimes are reported to the police because most are resolved elsewhere by the victims themselves or by the panoply of other types of organizations or groups involved in the regulation of behavior in cyberspace." Due to these reasons, Wall argues that the role of the public police in policing cybercrime should be understood as a small part of the networks of security within the cyberspace, and that the public police needs to forge new relationships with the other nodes within the network (Wall, 2011). It could be noted that many firms fall victims of these circumstances because of lack of policies and regulations or lack of awareness on how to handle cybercrime and their evidences.

2.1. Objectives of the Study

The main objective of this paper is to explore cybercrime cases in relation to organizational policies and the emerging issues.

3. Review of Related Literature

Many organizations prefer to appoint one incident response team member as the primary POC with law enforcement. This person should be familiar with the reporting procedures for all relevant law enforcement agencies and well prepared to recommend which agency, if any, should be contacted. (Scanfone, etal 2008).

Cabrera- Balleza (2008) raises the issue of laws on cybercrime lacking consideration of their social impact. Often pushed by the private sector to regulate intellectual property matters or by the State to enforce control and surveillance on citizens, it is uncertain whether women's rights stand to be protected or traded in this debate. Particularly with the acute lack of broader women's rights engagement, or even awareness, in this issue, claiming the boundaries and definition of the issues at stake – moving it beyond arguments of "terrorism", "national security" and "crimes against capitalism" - can be challenging. This then raises concerns on whether cybercrime laws will simply be mobilized to restrict communication rights of individuals and communities. As such, their different approaches and stances clearly demonstrate the difficulty of drawing a clear line between protection of women's rights from violation and empowering their status as users and definers of ICT and the information society.

Social engineering makes it even more difficult for a target to identify an attempted breach before it is too late. Although most users may recognize that viruses can infect their computer if they were to click on a link from an unrecognized email sender, riddled with spelling and grammatical errors, today, cyber-attacks can easily imitate trusted email addresses, text messages, media or websites. The information to make cyber-attacks appear trustworthy can be extracted from social media and other online personal or professional data (Sopohos, 2012).

Gabriel Tarde (1890; 1903) asserted that novel forms of criminal behavior are fostered through the superimposing of new practices onto traditional ones, often through technological advances or innovation. Due to the exponential growth of information technology in modern society, many traditional crimes are now being aided or abetted through the use of computers and networks, and criminality heretofore never conceived has surfaced because of the incredible capabilities of information systems.

Carrier and Spafford (2003) suggested a digital investigation process, which includes both physical and digital evidence investigation in one integrated process. The model consists of seventeen phases organized into five groups. The basic characteristic of the model is the separation of the investigation process to physical and digital crime scene investigation. Firstly, items found in the crime scene are handled as physical evidence using traditional investigation methods (e.g., fingerprints). If these items are source of digital evidence (e.g., computers, cell phones, peripherals) they are examined again according to digital crime scene investigation sub-phases and the results are added to the primary physical scene.

Employee training and awareness can be equally effective in mitigating malicious insider risks and damage. These cases often can be heralded by early warning signs such as poor work performance, issues with colleagues, disciplinary action, or living beyond their means; these are signs that employees and managers will notice, not IT security tools. This underscores the importance of training and awareness as a critical element of an insider threat management program, one that is integrated with current information security training and awareness, ethics training programs and the ombudsman process. This requires the participation of corporate functions: not just IT and information security, but also human resources, legal and physical security.

Threat Database, a repository of reported insider threat cases involving theft of IP using IT, IT sabotage, or fraud using IT, shows that 27% of the incidents in the database were detected by non-technical means. As an FBIinsider threat analyst explained this at the February 2013 RSA conference, "...the risk from insider threats is not a technical problem, but a people centric problem. So, you have to look for a people-centric solution. People are multidimensional, so what you have to do is take a multidisciplinary approach."

(http://www.darkreading.com/insider-threat/5-lessons-from-the-fbi-insider-threat-pr/240149745)

The growing role of digital evidence to support conventional criminal evidence also illustrates the need for law enforcement agencies to adopt new investigation methods. Up to now, most investigation models deal with only physical or only digital evidence, thus imposing a clear separation. In case of NIJ (2000), the crime scene investigation and Lee's *et al.* (2001) Scientific Crime Scene Investigation Model do not include specifications about digital evidence and their role in the documentation of a case.

Crime investigation theory is evolving as criminals find new ways to commit crimes. On the other hand, law enforcement investigations, commonly accepted procedures are implemented by most agencies around the world. For instance, a typical investigation includes the following basic steps (Vlachopoulos, 2007): Police are notified about a crime; after the necessary preparation an investigation takes place at the crime scene; the scene is secured, a thorough search for evidence is contacted and items considered as evidence are documented, bagged, labeled, collected and transported to the lab for further examination; finally, a police report refers to the results of the investigation.

Lee et al. (2001) presented the Scientific Crime Scene Investigation Model, which focuses on a systematic and methodical way of investigating a physical crime scene. Although the model refers only to physical crime scene investigation, it became a point of reference as many of its aspects can be used to search for digital evidence in an electronic crime scene investigation. The model refers only to the forensic part of an investigation, while issues such as preparation and exchange of information with other investigators are not addressed.

4. Results and Discussion

Government and firms alike has to develop policies to check the cybercrime, now that the adoption of automated systems is on the rise. In this view, the formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach.

In computer crime, witnesses are relatively rare since these offenses tend to occur behind closed doors (Rosoff et al., 2002). The only witnesses in most cases are those who commit the crimes either individually or collectively, and therefore other techniques to gather information must be utilized (Lyman,2002).

As the say goes "send a thief to catch a thief", organizations should engage the intelligent tools through their cyber security experts to gather future informed intentions of cyber criminals, this involved the use of advanced software and hardware to monitor cyber criminal's activities attempts on their own systems, in order to develop measures to counter them before final attack on the systems.

For evidence both traditional and digital form is a perquisite in a crime scene and since digital and physical evidence may coexist in a crime scene. Therefore, various items found in a crime scene may be valuable as both physical and digital evidence.

Many of the survey questions focus on the technologies organizations use to prevent and investigate cyber breaches, to improve organizational resilience once an attack compromises information system, and to improve overall organizational cyber security capabilities. Entities can find themselves in a constant cycle of attack and defend. As novel attack vectors and methods enter the ecosystem, the security industry develops new technologies and techniques to counteract these methods.

Cybercrimes continue to be costly. We found that the average annualized cost of cybercrime for 60 organizations in our study is $11.6 million per year, with a range of $1.3 million to$58 million. In 2012, the average annualized cost was $8.9 million. This represents an increase in cost of 26 percent or $2.6 million from the results of our cyber cost study published last year. (Ponemon Institute, October 2012.)

The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the information society and demands for more innovative drive in the uptake and protection against vulnerabilities. "One reason that many security-related incidents do not result in convictions is due to disconnect between the victim institution and the law enforcement agencies. The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected. Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures.

5. Conclusion and Recommendations

5.1. Summary of the Findings

The evidence presented in cases and literature review confirms that firms lack the solid existence of evidence gathering techniques for cybercrime. There also exist disconnect between law enforcement and policies governing cybercrime because of its dynamic nature, which in turn makes it difficult for cybercrime cases to see the light of the day in a court of law.

Many firms have witnessed heavy losses either report or behind the scene. Therefore, cyber surveillance and strategies need to be effectively employed, communicated and shared in a collaborative forum. Further the digital divide does not count in cybercrime because it operates in a global platform and can be committed anywhere everywhere. It is forms a mandatory requirement for the government, institution and the stakeholder to keep a breast with the latest requirement in terms of policies, standards, regulations and control mechanisms. In this regard, Brandl& Horvath (1991) discovered that the effort expended by law enforcement through investigative practices is positively related to victim satisfaction rates. That is, victims are more pleased with the police response when the department is able to demonstrate that due attention was given to the incident.

5.2. Conclusion

Based on the current trends, security experts must move from their traditional reactive nature to a more proactive one. Because this will be after the damage has been done, they need a way to be ahead of the threats. More importantly is being able to get a clear view of the existing vulnerabilities of systems and the setup configurations that make up today's ICT enterprise. Equal priority should be on automated systems which detects the vulnerabilities as they occur, and also enable the systems to remediate these vulnerabilities immediately, before the damage occurs. Prosecutors, Law enforcement authorities, and judiciary, require developed framework, sustainable mechanisms, comprehensive technical support and solid platform for the investigation to cybercrime.

5.3. Recommendation

- For the digital evidence to see the light of the day in a court of law, the evidence processes of acquisition, preservation, and analysis in a forensically safe manner and thus enable its presentation in court, specific equipment and software are

needed and personnel and professionals concerned must be trained to recognize, properly understand, and examine the evidence presented.

- New roles have to be allotted to existing agencies to deal with the needs for cyber security and the fight against cybercrime.
- The setup of organizational structure and functions for security and law enforcement have been given new platform to check the emerging challenges especially in the context of traditional criminal justice system.

6. References

i. Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmalleger& M. Pittaro (Eds.), Crimes of the internet: Prentice Hall. p. 286.
ii. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age: Polity Press.
iii. Policing Cybercrimes, (2011): Situating the Public Police in Networks of Security within Cyberspace. Police Practice & Research: An International Journal, 8(2), 183-205.
iv. Scanfone, K., Grance, T., &Masone, K. (2008). Computer Security Incident Handling Guide *NIST Special Publication*: National Institute of Standards and Technology. p. 2-6.
v. Ponemon Institute: *Cost of Cyber Crime Study: United States*, October 2012.
vi. Lee, H., Palmbach, T., and Miller, M. (2001), *Henry Lee's Crime Scene Handbook*, Academic Press, San Diego, ISBN: 0-12-440830-3.
vii. National Institute of Justice (2000), "Crime Scene Investigation, A guide for law enforcement", Research Report, *U.S. Department of Justice,* https://www.ncjrs.gov/pdffiles1/nij/178280.pdf, (Accessed 27 January 2012).
viii. Carrier, B. and Spafford, E. (2003), "Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vol. 2, No. 2.
ix. Rohini Tendulkar,(2013): IOSCO Staff Working Paper, Cyber-crime, securities markets and systemic risk.
x. Tarde, G. (Ed.). ([1890] 1903).Gabriel Tarde's laws of imitation. New York: Henry Holt.
xi. McGarrell, E. F., & Schlegel, K. (1993). The implementation of federally funded multi jurisdictional task forces: Organizational structure and interagency relationships. Journal of Criminal Justice, 21(3), 231-244.
xii. Brandl, S. G., & Horvath, F. (1991). Crime-victim evaluation of police investigative performance. Journal of Criminal Justice, 19(3), 293-305.
xiii. Lyman, M. D. (2002). Criminal investigation: the art and the science (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.
xiv. Vlachopoulos, K. (2007). Electronic Crime, NomikiVivliothiki, Athens, ISBN: 978-960-272-458-3.
xv. Rosoff, S. M., Pontell, H. M., & Tillman, R. (2002).Profit without honor: white-collar crime and the looting of America. Upper Saddle River, NJ: Prentice Hall.
xvi. Sopohos, 'Security Threat Report 2012: Seeing the threat through the hype', 2012
xvii. Barney Jopson, "Cybercrime link to outsourcing", Financial Times, 25 March 2013
xviii. Cabrera-Balleza, Mavic. 2008. *Finding a difficult balance: human rights, law enforcement and cyber vi*ndex.shtml?w=a&x=96169
xix. The standard newspaper – Fraudsters are becoming sophisticated with little chance of being caught or convicted, Saturday 5, July, 2014 pg. 8 by MwanikiMunuhe
xx. The standard newspapers: Kenya to install new cyber crime monitoring device, Monday, 11 June 2012.
xxi. The Standard newspaper: cybercrime on the rise, 5th July, 2014